

* * *

REMARKS

SUMMARY OF OFFICE ACTION AND SUMMARY OF RESPONSE

In the Office Action, Examiner cited a petition to correct inventorship and rejected same on the basis of CFR 1.48(a), requiring a statement from all added inventors of non-deceptive intent and consent of assignee(s).

Examiner rejected Claims 1-18 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Examiner rejected Claims 1-3, 5, 8, 9 and 11-13 under 35 U.S.C. 102(b) as being anticipated by Lorenz (US Patent 5,799,201).

Examiner rejected Claims 4, 6, 7 and 10 under 35 U.S.C. 103(a) as being unpatentable over Lorenz as applied to Claim 3 and further in view of Official Notice taken. Examiner also rejected Claim 14 under 35 U.S.C. 103(a) as being unpatentable over Lorenz as applied to Claim 8 and further in view of Official Notice taken.

In this Response, Applicant amends the specification, cancels old Claims 1-18 and provides new Claims in order to traverse Examiner's rejections.

PETITION TO CORRECT INVENTORSHIP

The patent application was filed on 02/04/99 with an unsigned declaration identifying two inventors (HOWARD, B. and ROBINSON, A.). Responsive to a Notice to File Missing Parts, Applicant provided an executed declaration dated February 3, 1999 identifying the original two inventors and four additional inventors (in total, HOWARD, B.; SELWYN, P.; LENNOX, S.; CAMERON, C.; LAMARCHE, M.; FLINDALL, L.; ROBISON, A; and FEGHALI, W.) and

an Assignment executed by the original two inventors and the additional four inventors. An additional statement regarding the corrected inventorship was provided signed by the two inventors identified in the original unsigned declaration.

It appears that Examiner considered the additional statement to be a petition to correct inventorship in the Office Action and subsequently rejected same. Based on the file history, Applicant submits that no such petition is required. While Examiner cited 37 C.F.R. 1.48(a), Applicant submits that 37 C.F.R. 1.48(a) is inapplicable to the executed declaration of record. As noted, Applicant filed only one executed declaration. Also, Applicant cites 37 C.F.R. 1.48(f)(1), which provides that:

“[i]f the correct inventor or inventors are not named on filing a nonprovisional application under §1.53(b) without an executed oath or declaration under §1.63 by any of the inventors, the first submission of an executed oath or declaration under §1.63 by any of the inventors during the pendency of the application will act to correct the earlier identification of inventorship”.

Based on the file history, Applicant traverses the rejection based on 37 C.F.R. 1.48(a).

Applicant understands that Examiner is prepared to withdraw his rejection based on 1.48(a) based on Examiner's telephone message of March 20, 2002 to Ms. Monica Rooney, a colleague in the office of the undersigned, wherein he confirmed the application of 37 C.F.R. 1.48(f)(1) to identify the executed declaration filed February 4, 1999 as the first executed declaration which can act to correct inventorship issues of the earlier unsigned declaration.

IN THE SPECIFICATION

The paragraphs beginning on page 3, line 13 and page 3, line 16 are amended to recite -- aspect-- rather than “object”. These amendments are made to correct informalities.

The paragraphs of the Summary of the Invention have been amended to conform to new Claims 19-33.

The paragraph beginning on page 4, line 26 is amended in lines 28 to recite -- buffer memory 3-- rather than memory buffer. It has also been amended in line 30 to recite --buffer memory 3-- rather than "memory" and in line 32 to recite --buffer memory 3-- rather than "memory 3". These amendments are made to correct informalities.

The paragraph beginning on page 5, line 18 is amended in lines 19 and 20 to recite -- buffer memory 5--. These amendments are made to correct informalities.

The paragraph beginning on page 5, line 25 is amended in lines 27 and 29 to recite -- ciphering processor 13-- rather than "ciphering processor". It also has been amended in line 28 to recite --processor 7-- rather than "processor". These amendments are made to correct informalities.

The paragraph beginning on page 6, line 3 is amended in line 3 to recite --buffer memory 5-- rather than "memory buffer 5" and in line 8 to recite --buffer memory 5-- rather than "memory 5". These amendments are made to correct informalities.

The paragraph beginning on page 6, line 11 is amended in line 12 to recite --data bus 2-- rather than "data bus". This amendment is made to correct informalities.

The paragraph beginning on page 7, line 13 is amended in line 14 to recite --the processed data is the same data in both functions-- rather than "the processed data is same data". It has also been amended in line 15 to recite --use of a single integrated processor-- rather than "use of single integrated processor". These amendments are made to correct informalities.

IN THE CLAIMS

Applicant's invention is directed to a system having a memory device having a memory buffer, a first access port connected to said memory buffer and a second access port connected to said memory buffer. The system also includes a data processing processor connected to the first

access port via a first bus and a ciphering processor connected to the second access port via a second bus. The first access port and the second access port each provide mutually independent access to the memory buffer. The second bus is not connected to the first bus. The data processing processor is adapted to receive the data and provide the data to the memory buffer over the first bus. The ciphering processor is adapted to retrieve the data from said memory buffer over the second bus, generate ciphered data from the data, generate integrity check information for the ciphered data and provide the ciphered data and the integrity check information to the memory buffer over the second bus.

Applicant cancels old Claims 1-18. New Claims 19-33 added herewith and are directed towards aspects of the invention. New Claims 19-30 are based on selected aspects defined in old Claims 1-18. New Claims 31-33 include aspects not present in old Claims 1-18.

Rejections under 35 U.S.C. 112, second paragraph

New Claims 19-33 particularly point out and distinctly claim the subject matter of Applicant's invention. Issues relating to lack of clarity of terms in old Claims 1, 2, 3, 4, 5, 8 and 10, to the extent any of such terms are used in new Claims 19-33, have been addressed in new Claims 19-33. Accordingly, Applicant traverses Examiner's objections to old Claims 1-18 under 35 U.S.C. 112, second paragraph.

Rejections under 35 U.S.C. 102(b) based on Lorenz (US Patent 5,799,201)

Lorenz provides a signal processor that operates its two processing units operating in parallel to process data. The signal processor is particularly adapted to computation of auto-correlation and cross-correlation functions and for FIR digital filtering.

Each claim of new Claims 19-33 is novel and is not anticipated by Lorenz. In the Office Action, Examiner cited Lorenz as anticipating old Claims 1, 3, 5, 8, 9 and 11-13. New Claims 19, 21, 24 and 29 are based on aspects of old Claims 8, 5, 9, and 13, respectively.

New Claim 19

First, new Claim 19 incorporates aspects of old Claim 8 and further includes a first and second bus where the second bus is not connected to the first bus. In contrast to the separated busses of new Claim 19, Lorenz does not teach having such a fully isolated bus structure. In fact Lorenz specifically teaches the opposite, where a first bus, which is connected to a first data processor, is also connected to a second bus connected to second data processor. See in Figure 1, bus system 1 connects data processor 4 and data processor 5 to memory 3. See also in Figure 2 where output busses from both data processors 4 and 5 are connected to both data buses 9 and 10. Lorenz does not therefore teach the isolation of the second bus as recited in new Claim 19.

Second, new Claim 19 further has a ciphering processor generating ciphered data and integrity check information for the ciphered data. Lorenz does not teach nor suggest using a data processor to generate and integrity check information for ciphered data. Instead, Lorenz teaches using data processor 4 and data processor 5 to perform computations in an algorithm to process signals such as voice signals (column 1, lines 13-35). More particularly, the data processing units 4 and 5 of Lorenz are described as being "particularly suitable for computing a multiplicity of n scalar products" (column 5, lines 4-5). The encryptor 35 shown in Figure 3 of Lorenz is not described as being one of the data processors 4 or 5 of Figure 2 and will therefore not provide the structure recited in new Claim 19. Additionally, the ALUs 14 and 18 shown in Figure 2 of Lorenz are not described as generating integrity check information and will therefore not provide the function recited in new Claim 19.

Based on the above first and second aspects of new Claim 19 and the limited teaching of Lorenz, Applicant submits that new Claim 19 is not anticipated by Lorenz.

Support for new Claim 19 is found in the specification on page 5 which describes the ciphering processor as connected to the memory via a data bus apart from the first data bus. The isolation of the second bus from the first bus is shown in Figure 2 which accompanies the description of the embodiment on page 5.

New Claim 21

New Claim 21, which depends from new Claim 19, incorporates aspects of old Claim 5 and includes in the ciphering processor an encryption module for generating the ciphered data and a message digesting module for generating the integrity check information.

Examiner rejected old Claim 5 as being anticipated by Lorenz citing in Lorenz, an encryptor 35 for generating ciphered data and ALUs 14 and 18 for performing verification operations. However, Applicant submits that Lorenz does not teach nor suggest that encryptor 35 (as shown in Figure 3) is specifically internally incorporated into either data processors 4 or 5, as provided in new Claim 21. Further, Lorenz does not teach or suggest using the ALUs 14 and 18 as a message digesting module to generate integrity check information, as provided in new Claim 21. Further still, as noted above, as new Claim 20 is novel over Lorenz, Applicant submits that new Claim 21, which depends on new Claim 20, is also novel over Lorenz.

New Claim 24

New Claim 24 incorporates aspects of old Claim 9 and depends from new Claim 23. New Claim 24 provides that the memory buffer includes dual port random access memory. As noted above, as new Claim 23 is novel over Lorenz, Applicant submits that new Claim 24, is also novel over Lorenz.

New Claims 25-28

New Claims 25-28 incorporate aspects of old Claims 15-18, respectively. The Examiner did not reject old Claims 15-18 based on the prior art made of record. Accordingly, Applicant submits that new Claims 25-28 are allowable.

New Claim 29

New Claim 29 incorporates aspects of old Claim 13 and depends from new Claim 19. New Claim 29 has the data processing processor operating asynchronously to the ciphering processor. As noted above, as new Claim 19 is novel over Lorenz, Applicant submits that new Claim 29, is also novel over Lorenz.

Rejections under 35 U.S.C. 103(a) based on Lorenz (US Patent 5,799,201) and Official Notice

Each Claim of new Claims 19-33 is not obvious based on Lorenz in view of Official Notice. In the Office Action, Examiner cited Lorenz and Official Notice as rendering old Claims 4, 6, 7, 10 and 14 obvious.

New Claim 20

New Claim 20, which depends from new Claim 19, incorporates aspects of old Claim 4 and includes in the ciphering processor an encryption module for generating the ciphered data and a hashing module for generating the integrity check information.

The Examiner took Official Notice that the encryption techniques recited in old Claim 4 are old and well known in the art of processor systems utilizing the features of Lorenz. However, it is respectfully submitted that the Examiner has provided no objective evidence of any teaching, motivation or suggestion for combining Lorenz with the Official Notice. The

Examiner is required to provide such evidence. *In re Lee*, 61 USPQ2d 1430 (CA FC 2002) states on pages 1433-4 that “[w]hen patentability turns on the question of obviousness, the search for and analysis of the prior art includes evidence relevant to the finding of whether there is a teaching, motivation, or suggestion to select and combine the references relied on as evidence of obviousness”. The rationale for combining references “must be based on objective evidence of record” and cannot be “resolved on subjective belief and unknown authority”.

Further, the *Manual of Patent Examining Procedure* (“MPEP”) sets out that the motivation to combine references must be explicitly set out. Section 2142 provides that:

If the examiner does not produce a prima facie case [of obviousness], the applicant is under no obligation to submit evidence of nonobviousness. ... To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The *teaching or suggestion to make the claimed combination* and the reasonable expectation of success *must both be found in the prior art*, and not based on applicant's disclosure. (emphasis added)

Additionally, section 2141 of *MPEP* requires that “[w]hen applying 35 U.S.C. 103, the following tenets of patent law must be adhered to: ... The references must be considered as a whole and must suggest the desirability and thus the obviousness of making the combination”. The Examiner must therefore produce “objective evidence of record” from the prior art showing motivation to combine these references and the reasonable expectation of success from such combination.

The Examiner has not provided any motivation or suggestion as to why Lorenz should be combined with the Official Notice. However, even if this were the case, it has been submitted above that Lorenz do not in any way teach or suggest the teachings of the invention as now

recited in new Claim 19. Accordingly, it is respectfully submitted that new Claim 20 is patentable over Lorenz as it ultimately depends from new Claim 19 which as been distinguished from Lorenz above.

New Claim 22

New Claim 22, which ultimately depends from new Claim 19, incorporates aspects of old Claim 6 and includes the encryption module performing DES or triple-DES encryption.

The Examiner took Official Notice that the encryption techniques recited in old Claim 6 are old and well known in the art of processor systems utilizing the features of Lorenz. The Examiner has not provided any motivation or suggestion as to why Lorenz should be combined with the Official Notice. However, even if this were the case, it has been submitted above that Lorenz do not in any way teach or suggest the teachings of the invention as now recited in new Claim 19. Accordingly, it is respectfully submitted that new Claim 22 is patentable over Lorenz as it ultimately depends from new Claim 19 which as been distinguished from Lorenz above.

New Claim 23

New Claim 23, which depends from new Claim 19, incorporates aspects of old Claim 7 and includes the hashing module being a HMAC hashing module for encoding the integrity check information within the ciphered data.

The Examiner rejected old Claim 7 as being unpatentable over Lorenz. Examiner took Official Notice that the hashing technique recited in old Claim 7 is old and well known in the art of processor systems utilizing the features of Lorenz. The Examiner has not provided any motivation or suggestion as to why Lorenz should be combined with the Official Notice. However, even if this were the case, it has been submitted above that Lorenz do not in any way teach or suggest the teachings of the invention as now recited in new Claim 19. Accordingly, it is

respectfully submitted that new Claim 23 is patentable over Lorenz as it ultimately depends from new Claim 19 which as been distinguished from Lorenz above.

New Claim 30

New Claim 30, which depends from new Claim 19, incorporates aspects of old Claim 14 and includes the data processing processor being clocked by a first clock source, the ciphering processor being clocked by a second clock source where the first clock source is asynchronous to the second clock source.

The Examiner rejected old Claim 14 as being unpatentable over Lorenz. The Examiner took Official Notice that the arrangement of clock sources recited in old Claim 14 is old and well known in the art of processor systems carrying out encryption processing. The Examiner has not provided any motivation or suggestion as to why Lorenz should be combined with the Official Notice. However, even if this were the case, it has been submitted above that Lorenz do not in any way teach or suggest the teachings of the invention as now recited in new Claim 19. Accordingly, it is respectfully submitted that new Claim 30 is patentable over Lorenz as it ultimately depends from new Claim 19 which as been distinguished from Lorenz above.

New Claims Having Additional Features Not Recited in the Old Claims

New Claim 31

New Claim 31 depends from new Claim 19. In new Claim 31, the system further includes a first communications port at which the data is received and a second communications port over which the data processing processor transmits the ciphered data. Since Lorenz does not teach or suggest the features recited in new Claim 19 listed above, it is respectfully submitted

that new Claim 31 is patentable over Lorenz as it ultimately depends from new Claim 19 which as been distinguished from Lorenz above.

Support for new Claim 31 is found in the specification at page 5 which provides that data arrives at the system at a first communications port 4a (page 5, lines 12-13) and is transmitted from the system from a second communications port 4b (page 5, lines 3-5). It also conforms to Figure 2 which shows the system having communications ports 4a and 4b.

New Claim 32

New Claim 32 depends from new Claim 31. In new Claim 32, the data received at the first communications port comprises fragments of a packet, the data processing processor stores the fragments in the memory buffer to assemble the packet and the ciphering processor generates the ciphered data from the assembled packet. Such aspects, are not taught in Lorenz. Accordingly, Applicant submits that new Claim 32 is not anticipated by Lorenz.

Support for new Claim 32 is found in the specification at page 5, lines 11-15 which states that packet fragments that "arrive at a first communication port 4a" are stored in the memory buffer. The specification further provides at page 5, lines 19-21 that "data within the buffer memory 5 is ciphered".

New Claim 33

New Claim 33 depends from new Claim 32. In new Claim 33, the system is disposed at a gateway between a private network and a public network in a secure virtual private network, the first communications port is connected one of the private network and the public network and the second communications port is connected to the other one of the private network and the public network. Such aspects, are not taught in Lorenz. Accordingly, Applicant submits that new Claim 33 is not anticipated by Lorenz.

Support for new Claim 33 is found in the specification on page 2, lines 1-10 which provides that in a secure virtual private network, the core network (private network) is coupled to the Internet (public network) via a gateway. The embodiment described on pages 5-9 is the system for ciphering data found at this gateway.

IN THE ABSTRACT

The paragraph of the Abstract of the Disclosure has been amended to conform to new Claims 19-33.

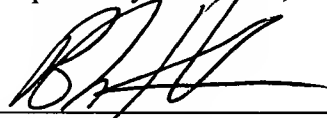
* * *

Attached hereto is a marked-up version of the changes made to the specification and claims by the current amendment. The attached pages are captioned "VERSION WITH MARKINGS TO SHOW CHANGES MADE."

No new matter has been added by way of this amendment. All amendments not specifically dealt with are to correct typographical errors and to correct informalities.

By way of the present amendment, this application is believed to be in condition for allowance and such action in due course is earnestly solicited. The Examiner is invited to contact the undersigned by telephone to discuss this case further, if necessary.

Respectfully submitted,



Robert H. Nakano
(Registration No. 46,498)
Blake, Cassels & Graydon
P.O. Box 25, Commerce Court West
Toronto, Ontario, M5L 1A9
Canada
(416) 863-2785 (Telephone)
(416) 863-2653 (Facsimile)

July 11, 2002
Date

A

VERSION WITH MARKINGS TO SHOW CHANGES MADE

In re. Application of: HOWARD, Brett L.
Serial No.: 09/244,203
Filed: 02/04/1999
Title: SYSTEM AND METHOD FOR CIPHERING DATA

Examiner: CALLAHAN, Paul E.
Art Unit: 2132
Confirmation No.: 3485

Atty's Docket No.: 53921/116

IN THE SPECIFICATION:

The paragraph beginning on page 3, line 13 is amended as follows:

In order to overcome the above limitations of the prior art, it is an aspect ~~object~~ of the invention to provide a method of ciphering data received by a gateway, the data ciphered absent accessing the memory buffer via the data bus.

The paragraph beginning on page 3, line 16 is amended as follows:

It is another aspect ~~object~~ of the invention to provide a method of encoding data for transmission via a wide area network-, the data ciphered and processed for determining integrity in parallel.

The paragraphs beginning on page 3, line 20 and page 3, line 26 are amended as follows:

~~In accordance with the invention there is provided a system for ciphering data stored within a memory buffer comprising:~~

~~an integrated processor retrieving data from the memory buffer, for ciphering the data, and for performing operations relating to verification of data integrity, the ciphering and the performed operations executed in parallel, the processor for providing processed data.~~

~~In accordance with the invention there is also provided a system for ciphering data comprising:
a memory buffer having a first port and a second port;
a plurality of communication ports;
a first processor in communication with the first port of the memory buffer and the plurality of communications ports;
a second processor in communication with the second port of the memory buffer, the second processor for ciphering data with in the memory buffer and for storing the data ciphered data within the memory buffer,
wherein data ciphering operations do not affect operations of the first processor.~~

In a first aspect, a system for ciphering data for transmission by a communication device is provided. The system includes a memory device having a memory buffer a first access port connected to the memory buffer and a second access port connected to the memory buffer. The system also has a data processing processor connected to the first access port via a first bus and a ciphering processor connected to the second access port via a second bus. The first access port and the second access port each provide mutually independent access to the memory buffer. The second bus is not connected to the first bus. The data processing processor is adapted to receive the data and provide the data to the memory buffer over the first bus. The ciphering processor is adapted to retrieve the data from the memory buffer over the second bus, generate ciphered data from the data, generate integrity check information for the ciphered data using the data and provide the ciphered data to the memory buffer over the second bus.

The ciphering processor may include an encryption module for generating the ciphered data and a hashing module for generating the integrity check information.

The ciphering processor may include an encryption module for generating the ciphered data and a message digesting module for generating the integrity check information.

The encryption module may include a DES encryption module for performing one of DES and triple-DES encryption.

The hashing module may include a HMAC hashing module for encoding the integrity check information within the ciphered data.

The memory buffer may include dual port random access memory.

The data processing processor may include a security module. The security module may retrieve a security context from memory. The security context may be used in generating the ciphered data.

The security module may determine a security context relating a source of the data or a destination for the ciphered data and may store the security context in the memory buffer. The security context stored may be accessible by the ciphering processor.

The data processing processor may include a security address module. The security address module may store an address associated with the security context in the memory buffer. The address may be based on the source of the data or the destination for the ciphered data.

The security module may provide an indication to the data processing processor when a security context is not present in the memory buffer.

The data processing processor may operate asynchronously to the ciphering processor.

The data processing processor may be clocked by a first clock source and the ciphering processor may be clocked by a second clock source. The first clock source may be asynchronous to the second clock source.

The system may further include a first communications port at which the data is received and a second communications port over which the data processing processor transmits the ciphered data.

The data received at the first communications port may include fragments of a packet. The data processing processor may store the fragments in the memory buffer to assemble the packet. The ciphering processor may generate the ciphered data from the assembled packet.

The system may be disposed at a gateway between a private network and a public network in a secure virtual private network. The first communications port may be connected to the private network or the public network and the second communications port may be connected to the other one of the private network and the public network.

The paragraph beginning on page 4, line 26 is amended as follows:

When the beginning of a packet is detected by the processor 7, a new file within the memory is created or a new portion of the memory is allocated for the packet. A ciphering circuit 8 then retrieves the file from the buffer memory buffer 3 via the data bus 2. The data within the buffer memory 3 is ciphered and data integrity information is generated for data integrity verification. The ciphered data is then stored in the buffer memory 3 via the data bus 2. When data is being secured for transmission via a wide area network, the integrity information is stored with the ciphered information. The processor 7 then retrieves the ciphered information from the buffer memory 3 via the data bus 2 and provides it to the second communication port 4b.

The paragraph beginning on page 5, line 18 is amended as follows:

When the beginning of a packet is detected by the processor 7, a new file within the buffer memory 5 is created. A ciphering processor 13 then retrieves the file from the buffer memory buffer 5 via a second other data bus. The data within the buffer memory 5 is ciphered and data integrity information is generated for data integrity verification. The ciphered data is then stored. When data is being secured for transmission via a wide area network, the integrity information is stored with the ciphered information. The processor 7 then retrieves the ciphered information and provides it to the second communication port 4b.

The paragraph beginning on page 5, line 25 is amended as follows:

Clearly, processing of a packet requires at least two data bus operations, half of the prior art implementation. Thus, using a system as described herein, performance is improved substantially. Also, since the ciphering processor 13 operates independent of the processor 7 and of the data bus 2, it is possible to clock the ciphering processor 13 independent of the other processor 7. Therefore, when ciphering operations prove to be a bottleneck, a faster ciphering processor 13 is used. Alternatively, when the processor 7 is the bottleneck, a faster processor 7 is used.

The paragraph beginning on page 6, line 3 is amended as follows:

The buffer memory buffer 5 is preferably formed of dual ported random access memory. Of course, when reduced performance is acceptable, a random access memory arbitration circuit (not shown) is used to arbitrate access to the random access memory making it function similarly

to dual ported memory. In essence, either the ciphering processor 13 or the processor 7 are switched to drive the memory circuitry. By using true dual ported random access memory, both the processor 7 and the ciphering processor 13 can access the buffer memory 5 simultaneously. This effectively eliminates operations of one processor from affecting operation the other.

The paragraph beginning on page 6, line 11 is amended as follows:

At least four memory access operations are required to process a packet; however, they are now performed two on the data bus 2 and two on a second other data bus. This is highly advantageous as described above.

The paragraph beginning on page 6, line 14 is amended as follows:

The implementation of ciphering and data integrity operations in parallel improves system performance. Prior art systems perform one operation and then the other. Implementation of the two operations in parallel requires some set up operations and a final operation of the data integrity processing. That said, it reduces two sequential operations to one operation equal to the greater of the two. The improved efficiency allows for a ciphering processor 13 having reduced performance and yet capable of achieving a same overall data throughput.

The paragraph beginning on page 7, line 13 is amended as follows:

Thus, it is clear that implementation of these functions in parallel within a single ciphering processor is advantageous. Further, since the processed data is the same data in both functions, the use of a single integrated processor reduces memory access operations since the

same data is used by each of the processing portions of the ciphering processor 13. This has an added advantage of increasing performance through reduced access to external memory.

The paragraph beginning on page 7, line 18 is amended as follows:

When a packet is ciphered according to the invention and results in a packet that is too large for transmission via a network, the packet is fragmented. Such a packet, ~~having~~ has two fragments. In this case, the receiving end may be optimized to process paired fragments.

The paragraph beginning on page 8, line 21 is amended as follows:

The ciphering system in the form of an ASIC or an FPGA includes means to look up the security association determined by the host processor. The security association is, for example, a the context in which a packet is to be ciphered including keys and ciphering algorithms. The host processor includes means for determining a security association and for storing the determined security association in a location accessible by the ciphering processor. For example, the security association is stored in the dual ported RAM. Alternatively, the security association is stored in memory within the ciphering processor.

The paragraph beginning on page 9, line 1 is amended as follows:

In use, the ciphering processor receives a packet. An address for the packet is determined and a security context associated with the packet address is located when present. The located security context is then used to cipher the packet. Alternatively, when the security context is not present, a signal is provided to the host processor which then determines and stores a security

context for the packet. Such a method shifts much of the packet processing requirements from the host processor to the ciphering processor is in an efficient and cost effective manner.

IN THE CLAIMS

Claims 1-18 have been cancelled.

Claims 19-33 have been added.

IN THE ABSTRACT

The paragraph of the Abstract of the Disclosure has been amended as follows:

~~There is provided a system and method for encoding and decoding of secured data. Decoding of secure data within a receive buffer is performed by a processor dedicated to that function. The processor accesses the data from a data port other than the bus used by a first processor. In this fashion, the data bus of the first processor is free for other operations while ciphering operations are underway. Also, the data is ciphered and hashed for data integrity in parallel to improve performance. Because the dedicated processor is not in direct communication with the data bus, it is clocked by a different clock and can therefore be designed economically to meet throughput requirements of a given system.~~

A system for ciphering data for transmission by a communication device is provided. The system includes a memory device having a memory buffer a first access port connected to the memory buffer and a second access port connected to the memory buffer. The system also has a data processing processor connected to the first access port via a first bus and a ciphering processor connected to the second access port via a second bus. The first access port and the second access port each provide mutually independent access to the memory buffer. The second bus is not connected to the first bus. The data processing processor is adapted to receive the data

and provide the data to the memory buffer over the first bus. The ciphering processor is adapted to retrieve the data from the memory buffer over the second bus, generate ciphered data from the data, generate integrity check information for the ciphered data using the data and provide the ciphered data to the memory buffer over the second bus.

BLAKE, CASSELS & GRAYDON

PARCEL LIST

TO: THE COMMISSIONER OF PATENTS AND TRADEMARKS

Disbursement Code 53

DATE: July 11, 2002

U.S. Patent Parcel No.: 1657

Cheque Number: 8073284

Waybill No.: W6684235218

Client Name <u>Application No.</u>	PIC	Client/Matter No. (Dkd)	Amount	Description	Date
Alcatel Canada Inc. 09/244,203	RNA	53921/116	\$920.00 (U.S.)	Response & Amendment Petition for Extension of time.	Jul. 15, 2002
TOTAL:			\$920.00 (U.S.)		